REMARKS

This is in response to the Office Action dated September 28, 2009. In view of the above amendments and the following remarks, reconsideration of the rejection and further examination are requested.

Rejection under 35 U.S.C §101:

Claims 35, 37, and 41 have been rejected under 35 U.S.C §101 as being directed to non-statutory subject matter. This rejection is submitted to be inapplicable to the claims, as amended, for the following reasons.

Claim 35 has been amended to recite that the content playback method is performed using a processor and that the encrypted content is recorded on a computer readable recording medium. These two machines (the processor and the computer readable recording medium) are sufficient to positively "tie" the method to a "particular machine" as required in Bilski (see *In re Bilski*, 88 USPQ2d 1385). As a result, claim 35 qualifies as a statutory process under 35 U.S.C §101.

Claim 37 has been amended to recite "the computer program stored in a computer readable storage medium, wherein the computer program, when executed, causes the computer to perform steps of", as suggested by the examiner. As a result, claim 37 is not "software per se", and as a result, qualifies as statutory subject matter under 35 U.S.C §101.

Claim 41 has been amended to recite "a computer readable recording medium" that stores the encrypted content. The recording medium is now limited to a computer readable storage medium, as suggested by the examiner. As a result, claim 41 qualifies as statutory subject matter under 35 U.S.C §101.

Rejection under 35 U.S.C §102(b):

Claims 1-5, 7, 8, 10-28, and 30-42 have been rejected under 35 U.S.C §102(b) as being anticipated by Sako (US Pub. 2004/0030909). This rejection is submitted to be inapplicable to the claims, as amended, for the following reasons.

Claim 1 recites a content playback device including, in part, a judgment unit operable to acquire, from a source other than the recording medium, contract information relating to a

contract for use of the encrypted content, and judge, based on the acquired contract information, whether the encrypted content is permitted to be used, and a generation unit operable to generate a content key based on the read media information and the acquired contract information, if the encrypted content is judged as being permitted to be used.

According to the above features as recited in claim 1, the content key is generated based on the media information read from the recording medium and the contract information acquired from a source other than the recording medium, and the encrypted content recorded on the recording medium is decrypted using the generated content key. This prevents the unauthorized decryption of content on recording media that can occur when the content key can be generated merely with the use of the media information recorded on the recording media, because the content key is generated based on the media information read from the recording media and the contract information acquired from a source other than the recording medium. The above features as recited in claim 1 are not disclosed or suggested by Sako.

Sako discloses a recording medium reproducing method. In Sako, the content key data and the data with respect to DRM have been encrypted. The encrypted content key data and the encrypted data with respect to DRM have been recorded on the optical disc D (see paragraph 28). When the encrypted data is decrypted by the decryptor 51, the decryptor 51 decrypts the encrypted data with respect to DRM. As a result, the data with respect to DRM is extracted. The encrypted content key data and the encrypted data with respect to the DRM, which are read from the optical disc D by the optical pickup (not shown), are supplied to a decryptor 52. The decryptor 52 decrypts the encrypted content data and the encrypted data with respect to the DRM using key locker key data KL_Key, obtains content key data CON_Key as output data, and obtains the data with respect to the DRM (see paragraph 29).

Thus, Sako discloses that encrypted data with respect to DRM and an encrypted content key have been recorded on a recording medium. The encrypted data with respect to DRM and the encrypted content key are decrypted by a decryptor, and as a result, data with respect to DRM and a content key are generated. The content key is used to decrypt an encrypted content. The data with respect to DRM is used to judge output of the decrypted content. However, Sako does not disclose that the media information is read from the recording medium and contract information is acquired from a source other than the recording medium, and further that the content key is generated based on the *read media information and the acquired contract*

information. In contrast, Sako merely discloses the encrypted content key data and the encrypted data with respect to DRM have been recorded on the optical disc, and the encrypted content key data and the encrypted data with respect to DRM are decrypted, thereby generating the content key data and the data with respect to DRM. Thus, when an attacker analyzes the information recorded on the optical disc of Sako and acquires the content key and the data with respect to DRM without authorization, there is a risk that the content will be decrypted and the copyright of the content will be violated. Therefore, Sako does not disclose or suggest a judgment unit operable to acquire, from a source other than the recording medium, contract information relating to a contract for use of the encrypted content, and judge, based on the acquired contract information, whether the encrypted content is permitted to be used, and a generation unit operable to generate a content key based on the read media information and the acquired contract information, if the encrypted content is judged as being permitted to be used, as recited in claim 1. As a result, claim 1 is not anticipated by Sako.

Claims 35 and 37 are not anticipated by Sako for reasons similar to those discussed above with regard to independent claim 1. Specifically, claims 35 and 37 both recite acquiring, from a source other than the recording medium, contract information relating to a contract for use of the encrypted content, and judging, based on the acquired contract information, whether the encrypted content is permitted to be used, and generating a content key based on the read media information and the acquired contract information, if the encrypted content is judged as being permitted to be used. Since the above features of claims 35 and 37 are not disclosed or suggested by Sako, claims 35 and 37 are not anticipated by Sako.

Claim 41 discloses, in part, first encrypted content protected by a first protection method and protection method information showing the first protection method, in correspondence with each other, and second encrypted content protected by a second protection method different from the first protection method and protection method information showing the second protection method, in correspondence with each other.

According to the above features as recited in claim 41, the first encrypted content is protected by a first protection method, and the second encrypted content is protected by a second protection method. Because these encrypted contents are respectively protected by two types of protection methods which differ from each other, if one of the protection methods is attacked and the protection is impaired, the other encrypted content is protected by the other protection

method. The above features as recited in claim 1 are not disclosed or suggested by Sako.

Sako discloses that medium bind key data MB_Key which has been read from the optical disc D by the optical pickup (not shown) is supplied to the hash calculating portion 53. Likewise, medium key block data MKB which has been read from the optical disc D is supplied to a calculating portion 54. Device key data DEV _Key stored in a controller or the like of the apparatus is supplied to the calculating portion 54. The calculating portion 54 calculates medium key block data MKB and device key data DEV _Key and generates key data MKB _Key. The hash calculating portion 53 obtains a hash value of medium bind key data MB_Key and key data MKB_Key as key locker key data KL_Key. The hash calculating portion 53 supplies key locker key data KL _Key to the decryptor 52. With key locker key data KL _Key, the decryptor 52 decrypts the content key data and the data with respect to DRM and obtains content key data CON_Key (see paragraph 32). When the encrypted content data is decrypted by the decryptor 51, the data with respect to DRM is extracted. Decrypted content data, corresponding to the data with respect to DRM, which is output from the decryptor 51 is controlled. As a result, reproductions and copies of the decrypted content data are restricted (see paragraph 29).

Thus, according to Sako, key data MKB-Key is generated from media key block MKB and device key data DEV _Key. Next, key locker key data KL_Key is generated from medium key bind key data MB_Key and key data MKB_Key. Next, the encrypted content key is decrypted to generate the content key CON_Key using the key locker key KL_Key. Next, the encrypted content is decrypted using the content key CON_Key, whereby the content is obtained. Playback on the obtained content is controlled by data with respect to DRM. However, *Sako does not disclose storing first encrypted content and second encrypted content*. In Sako, in order to control decryption and playback of one content recorded on the optical disc D, medium key block data, medium bind key data, and DRM are used. According to the structure of Sako, if the protection method using the media key block and the medium key bind key data is attacked, the content may be acquired in an unauthorized manner, violating the right of the right holder. The data with respect to DRM is used for controlling playback of the content. The encrypted content is not protected by DRM. The encrypted contents are *not protected by two different protection methods*. Consequently, when one of the protection methods is attacked, Sako does not disclose that a second encrypted content is protected by the other protection method. Therefore, Sako does not disclose or suggest first encrypted content protected by a first

protection method and protection method information showing the first protection method, in correspondence with each other, and second encrypted content protected by a second protection method different from the first protection method and protection method information showing the second protection method, in correspondence with each other, as recited in claim 41. As a result, claim 41 is not anticipated by Sako.

Claims 2-5, 7, 8, 10-28, and 30-34 are either directly or indirectly dependent on independent claim 1. Claim 36 is dependent on independent claim 35. Claim 38 is dependent on independent claim 37. Claim 42 is dependent on independent claim 41. As a result, claims 1-5, 7, 8, 10-28, and 30-42 are allowable over Sako.

Rejection under 35 U.S.C §103(a):

Claims 6, 9, and 29 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Sako (US Pub. 2004/0030909) in view of Peinado (US 6,772,340). This rejection is respectfully traversed and submitted to be inapplicable the claims for the following reasons.

Claims 6, 9, and 29 are ultimately dependent on independent claim 1, discussed in detail above.

Peinado discloses, according to Figure 18, that the authoring tool 18, authoring such digital content 12, or the content server 22, serving such digital content 12, selects a key ID for the digital content 12 (step 1801). The content server 22 then employs the selected key ID as an input to a function f(), perhaps along with a secret 'seed' (step 1803). The output of such function f() is then employed as the symmetric encryption and decryption key (KD) for the digital content 12, f(key ID, seed) ---> key (KD), (step 1805), and the digital content 12 is therefore encrypted according to the key (KD) (step 1807). Such encrypted digital content 12 may thereafter be distributed to a user's computing device 14 (step 1809) (see col. 41, lines 49-63).

However, it is apparent that Peinado fails to disclose or suggest the features lacking from Sako discussed above with regard to independent claim 1. Accordingly, no obvious combination of Sako and Peinado would result in, or otherwise render obvious under 35 U.S.C. §103(a), the features recited in claims 1 and 18. As a result, claims 1 and 18 are patentable over the combination of Sako and Peinado.

Because of the above-mentioned distinctions, it is believed clear that claims 1-42 are allowable over the references relied upon in the rejection. Furthermore, it is submitted that these

distinctions are such that a person having ordinary skill in the art at the time of the invention would not have been motivated to combine the references of record in such a manner as to result in, or otherwise render obvious, the present invention as recited in 1-42. Therefore, it is submitted that claims 1-42 are clearly allowable over the prior art of record.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance. The examiner is invited to contact the undersigned by telephone if it is felt that there are issues remaining which must be resolved before allowance of the application.

Respectfully submitted,

Masaya YAMAMOTO et al.

/Allen N. Doyel/
2009.12.28 14:24:47 -05'00'

By _____
Allen N. Doyel
Registration No. 60,391
Agent for Applicants

AND/MSH/clw
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
December 28, 2009